UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JESSE STRIVELLI, **Plaintiff,** **v.** **JOHN DOE,** **Defendant.**	**PLAINTIFF'S MOTION FOR EXPEDITED DISCOVERY** **No.**

Plaintiff Jesse Strivelli, an individual, by and through his undersigned counsel and pursuant to Federal Rules of Civil Procedure 16(b), 26(d)(1), 30(a)(2)(A)(iii), hereby requests an order permitting him to engage in expedited discovery from third parties to enable Plaintiff to obtain documents and information pertaining to the identity of defendant John Doe, an online scammer who has stolen cryptocurrency and other digital assets from Plaintiff and continues to do so on an ongoing basis.

I. FACTS

Plaintiff is the owner of two digital wallets which contain 37 "smart contracts" which automatically generate revenue for Plaintiff in the form of cryptocurrency. See Declaration of Plaintiff Jesse Strivelli dated April 7, 2022 ("Strivelli Decl.") ¶¶3-4, submitted herewith. The revenue-generating smart contracts are tied to Plaintiff's wallets, and presently cannot be moved. Strivelli Decl. ¶13. Until he became the victim of a "phishing" scam by Defendant, Plaintiff had earned over $177,000 from his investment in the smart contracts. Strivelli Decl. ¶5.

On December 28, 2022 John Doe contacted Plaintiff in a chat group where Plaintiff was seeking help with a technical problem. Strivelli Decl. ¶¶8-9. John Doe offered to help. Plaintiff

permitted John Doe access to his computer using screen-sharing software called Microsoft TeamViewer. Strivelli Decl. ¶11. Once John Doe had access to Plaintiff's computer, John Doe hunted around in Plaintiff's computer, located the passcodes for Plaintiff's digital wallets, and stole them. Strivelli Decl. ¶¶12-13.

The theft of the passcodes ("keys") had two results:

First, John Doe immediately accessed Plaintiff's wallets and drained all the moveable assets, mostly Plaintiff's cryptocurrency, and were worth nearly $70,000. Strivelli Decl. ¶6. John Doe transferred some of these assets to a wallet ("John Doe Wallet 1") with the address:

0x1154b334285aE2AA67Cd94268Fe8c4d58e53e283.

Other stolen assets were transferred to a wallet ("John Doe Wallet 2") with the address:

0x7e317e89fd677d4c986a7f45b112494bda25fe43.

See Coinfirm Report On Fraud Event, dated April 7th, 2022 ("Coinfirm Report") at §2.2, submitted herewith.

Second, John Doe continues to access Plaintiff's wallets and steal the revenue generated by Plaintiff's smart contracts. Strivelli Decl. ¶19. The smart contacts cannot presently be moved out of Plaintiff's wallets and continue to generate revenue. Strivelli Decl. ¶¶ 13, 16-20. When the smart contracts generate revenue, they do so by generating a digital token which remains in the wallet until Plaintiff (or John Doe) accesses the wallet and removes the token.

Since the theft of the passcodes, Plaintiff and John Doe race to grab the tokens before the other one does. Plaintiff often loses the race. Since John Doe stole access to Plaintiff's wallets, $34,592 of smart contract revenue has gone to John Doe, and $14,090.31 to Plaintiff. Strivelli Declaration ¶¶19-20. John Doe has accessed Plaintiff's wallet to steal tokens at least 16 times. Strivelli Decl. ¶19.

In addition, there is a transaction cost to removing the tokens, called a "gas fee." Before the theft, Plaintiff would access his wallets approximately once a month and collect the tokens that had been generated in a single transaction. Strivelli Decl. ¶¶17-18. Now that he has to constantly access the wallet and collect the tokens whenever he can, Plaintiff has paid $37,910.44 in gas fees since the theft. Strivelli Decl. ¶21.

Lastly, at some point in 2022 the smart contracts will become transferable. Strivelli Declaration ¶22. This means that instead of just stealing the tokens, John Doe will have the opportunity to steal the contracts themselves.

II. THE REQUESTED EXPEDITED DISCOVERY

Plaintiff requests expedited discovery in order to serve subpoenas on cryptocurrency exchanges to identify John Doe, John Doe's accounts, and to identify any accounts where Plaintiff's stolen assets are located.[1]

Cryptocurrency exchanges maintain wallets and transactional accounts for their customers. The exchanges are required to keep information concerning the identity of the customers. John Doe Wallets 1 and 2 are private wallets, which means they are not associated with any identifiable cryptocurrency exchange.

"Defrauded cryptocurrency funds are typically passed through complex layering/mixing schemes aimed at concealing the trail of funds." *See* accompanying *Coinfirm Report on Fraud Event* dated April 7, 2022 ("Coinfirm Report") §5.1. Using five different accounting methodologies and tracking the movement of cryptocurrency and assets into and out of John Doe's known wallets, Plaintiff and Coinfirm, his expert consultant company, have identified several

[1] Plaintiff is also seeking a temporary restraining order without notice forbidding John Doe from continuing to access Plaintiff's wallets and ordering the exchange to freeze any of John Doe's wallets that can be identified.

wallets associated with cryptocurrency exchanges that have a high likelihood of being owned or controlled by John Doe. This is because the identified wallets send or receive cryptocurrency to John Doe's known wallets or the identified wallets have held or currently hold some of Plaintiff's stolen assets.

Coinfirm's analysis begins with the wallets into which Plaintiff's stolen assets were originally moved, John Doe Wallets 1 and 2. Coinfirm Report §2.2. Coinfirm has also identified another wallet, which has the address **9e1eba63a08b7aaf94918378dbb0d3b5eb599292** and is highly likely to be owned or controlled by John Doe ("John Doe Wallet 3"). This is because John Doe Wallet 1 has both sent and received assets from John Doe Wallet 3. Coinfirm Report §§ 4.4.3, 4.4.4.

These cryptocurrency exchanges will have the identity of the owners of the wallets that plaintiff and his expert have identified. The exchanges are also likely to have useful information about the location of Plaintiff's stolen assets. Accordingly, Plaintiff requests leave to serve subpoenas on the following exchanges to obtain information on the accounts associated with John Doe.

Coinbase Global, Inc.

John Doe Wallet 1 *and* John Doe Wallet 3 received assets from a Coinbase wallet with the address: **88dcdd4a0a58b7e2208805d547043c37dca2b6dc** on seven occasions. Coinfirm Report §§4.1(4); 4.4.2; 4.4.3; 4.4.4. In addition John Doe Wallet 2 received assets from two Coinbase wallets: **3cd751e6b0078be393132286c442345e5dc49699** and **b5d85cbf7cb3ee0d56b3bb207d5fc4b82f43f511.** Coinfirm Report §§4.1(4); 4.4.1.

StrongBlock, Inc.

John Doe deposited stolen assets from John Doe Wallet 1 to a StrongBlock account with the address **fbddadd80fe7bda00b901fbaf73803f2238ae655** twelve times. Coinfirm Report §4.3.1.2. These transactions were likely the result of the ongoing theft of the smart contract revenue since they occurred after the December 28, 2021 theft. Accordingly, it is likely that John Doe owns or controls this wallet. Coinfirm has also separately identified this wallet as one holding some of Plaintiff's stolen assets. *Id*. at §4.3.1 - 4.3.1.3.

gate.io (Gate Technology Incorporated)

John Doe deposited stolen assets from John Doe Wallet 2 into Gate.io account **b629e56db877ef4a13ceb6fa8ccd51344126c08c.** Coinfirm Report §4.1(3); App'x 1. John Doe did this after converting some of Plaintiff's stolen assets into $3500 of U.S. dollar stable coins. Coinfirm Report §§4.3.1.2; 4.3.1.3. It is likely that the Gate.io account referenced above is one of John Doe's trading accounts. Coinfirm has also separately identified this address as one holding some of Plaintiff's stolen assets. *Id*. at §4.3.1 - 4.3.1.3.

KuCoin (Mek Global Limited)

John Doe Wallet 3 has received funds from KuCoin account **f16e9b0d03470827a95cd fd0cb8a8a3b46969b91** on three occasions. Coinfirm Report §4.4.3.

Crypto.com

John Doe Wallet 2 received assets from a Crypto.com account bearing the address **46340b20830761efd3283 2a74d7169b29feb9758**. Coinfirm Report 4.1(4).

FTX Trading Limited

John Doe deposited stolen assets from John Doe Wallet 2 into Gate.io account **37b2b6801e6731f5bcc790463da51be360a205cb.** Coinfirm Report §4.1(3); App'x 1. Coinfirm has also separately identified this address as one holding some of Plaintiff's stolen assets. *Id*. at §4.3.1 - 4.3.1.3.

OpenSea, Inc.

John Doe sold an NFT (Strong Bronze #2227) from John Doe Wallet 1 to a buyer on December 28th, 2021 on the OpenSea exchange. The buyer's wallet address is **46683e62d890e8b4e49c7260ecc31eae60b416ec**. Coinfirm Report §4.2. It is possible that John Doe is the buyer and transferred the NFT for cryptocurrency in order to obscure the trail of the stolen assets, but it is more likely that the buyer is a separate party. Plaintiff requests permission to serve discovery on OpenSea to obtain the identity of the buyer and any information OpenSea might have concerning John Doe, such as if any of the wallets associated with John Doe are linked to any OpenSea accounts. In addition, discovery of the identity of the holder of the buyer's wallet will permit the notification of the buyer of the stolen nature of the NFT.

The subpoenas Plaintiff intends to serve on the exchanges will be narrowly tailored to discover these facts. For the exchanges, the subpoenas will seek:

i. All documents related to WALLET ADDRESS including account opening and closing, the identity of the account holder, all proofs of identification (such as government-issued photo ID), date of birth, Social Security Number, telephone number, electronic mail address, residential/mailing address, and Know Your Customer ("KYC") and Anti- Money Laundering ("AML") information compiled by EXCHANGE.

ii. All documents related to any other EXCHANGE accounts controlled by the individual(s) identified in (i).

iii. All documents related to transactions, funding, registered funding sources (i.e., bank accounts or other sources of funding tied to JOHN DOE's account[s]), and account holdings, including but not limited to transactions into or out of the following wallet address: (the "Wallet Address").

iv. Correspondence with, or related to, the individual(s) identified in (i).

Subpoena on Microsoft Corporation

John Doe used a Microsoft product, TeamViewer, to access Plaintiff's computer. Strivelli Decl. ¶11. Plaintiff will provide Microsoft with the machine ID for John Doe's computer, and request that Microsoft provide any information on the identity or location of the owner of the computer.

III. LEGAL ARGUMENT

This Court has broad discretion over discovery matters. *In re Fine Paper Antitrust Litig.*, 685 F.2d 810, 817 (3d Cir. 1982) ("Matters of docket control and conduct of discovery are committed to the sound discretion of the district court.").

Courts in the Third Circuit generally use the "good cause" test to evaluate requests to issue early discovery, including discovery seeking the identity of John Doe defendants. *See Strike 3 Holdings, LLC v. Doe*, No. 1:18-cv-2674-NLH-JS, 2020 U.S. Dist. LEXIS 114598, at *10 (D.N.J. June 30, 2020) (permitting expedited issuance of subpoena to ISP to ascertain identities of John Doe defendants and citing cases).

In *Strike 3 Holdings*, a similar case to this one, the court set forth a "non-exclusive list of factors courts typically examine in conducting the good cause analysis … (1) the timing of the

request in light of the formal start to discovery; (2) whether the request is narrowly tailored; (3) the purpose of the requested discovery; (4) whether the discovery burdens the defendant; and (5) whether the defendant can respond to the request in an expedited manner. *Id*. at *10-11.

Plaintiff's request for expedited discovery satisfies these factors.

First, the timing of plaintiff's request is the only possible timing because formal discovery following a 26(f) conference is not possible without identifying the defendant.

Second, plaintiff's request is narrowly tailored. Based on Coinfirm's analysis, the subpoenas will seek information concerning a small group of wallets and accounts that have been shown to be owned by, or closely related to, John Doe. Further, the subpoenas seek information necessary to identify and notify the defendant of these proceedings, and to identify wallets that may contain Plaintiff's assets which will be the subject of Plaintiff's preliminary injunction motion. Indeed, without this discovery, Plaintiff cannot request a preliminary injunction with sufficient specificity.

Third, the purpose of this discovery is to identify the party who allegedly stole and continues to steal Plaintiff's digital assets. As the court in *Strike 3 Holdings* stated, "Binding Circuit-level precedent advises courts to grant limited discovery in circumstances where a plaintiff may not otherwise have access to means for identifying John Doe defendants." *Id*. at 22-23 (citing *Alston v. Parker*, 363 F.3d 229, 233 n.6 (3d Cir. 2004)).

Fourth and fifth, this request for discovery does not burden the defendant since it is addressed to third parties. In addition, this discovery does not pose a significant burden to the exchanges, since plaintiff and coin firm have narrowed the number of wallets and accounts to a small number that are likely to yield the requested evidence.

Other federal courts have authorized expedited discovery to serve subpoenas on cryptocurrency exchanges to identify defendants. *See Williams v. Doe*, No. 6:21 -cv- 03074 (W.D. Mo. Dec. 7, 2021) (Attached as Exhibit B to the Declaration of Adam Gonnelli submitted herewith); *Heissenberg v. Doe*, No. 21-CIV-80716 (S.D. Fla. Apr. 23, 2021) (Attached as Exhibit A to the Gonnelli Declaration); *Singulardtv v. Doe*, No. 1:21-cv-060000, 2021 U.S. Dist. LEXIS 164866 (S.D.N.Y. Aug. 16, 2021).

IV. CONCLUSION

Because it will be impossible to identify the defendant or frame a proper request for an injunction otherwise, Plaintiff's request for expedited discovery should be granted.

Respectfully submitted,

Dated: April 8, 2022

Law Office of Adam R. Gonnelli, L.L.C.

By_____
Adam Gonnelli
707 Alexander Road
Building 2, Suite 208
Princeton, New Jersey 08540
phone: (917) 541-7110
adam@arglawoffice.com

Attorneys for Plaintiff